REMARKS/ARGUMENTS

Claim Amendments

The Applicant has amended claims 1-2, 5 and 7. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-7 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1 and 3-7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Mamros et al. (hereinafter Mamros) US Patent Number 6,360,269 in view of Patel et al. IP Security Working Group, Internet Draft, Revised SA negotiation mode for ISAKMP/Oakley. Intel Corporation (hereinafter Patel). The Applicant respectfully traverses the rejection of these claims.

The Applicant's invention discloses a method and apparatus for encrypting VOIP transmissions. A secure channel is used for creating keys needed to encrypt the VOIP traffic that is sent as an encrypted stream without using the headers normally associated with encrypted exchanges. For small VoIP packets a header overhead becomes impractical. Since the VOIP transmissions are not subjected to a complete IPSec procedure, after removing the headers there is not a protected second channel and the resulting packets do not include IPSec headers. For voice transmission this is acceptable but for other data it is not the case. In the case of VoIP, because of the sized of the voice packets, the absence of IPSec headers reduces unnecessary overhead and headers are not needed because voice data can tolerate some replay.

The Applicant respectfully directs the Examiner's attention to amended independent claim 1.

> 1. (Currently Amended) A method of sending streamed data over an IP network from a first node to a second node, the method comprising:
>
> using from the first a first protocol to establish a first security association (SA1) between the first and second nodes;
>
> using the first protocol to establish a first security association (SA1) over a second protocol between the first and second nodes:

modifying the second security association (SA2) by using selected components of the second protocol for providing encryption at the first node of the streamed data between the first and second nodes;

constructing datagrams containing segments of the encrypted streamed data in the datagram payload, the datagrams including a reduced overhead corresponding to the selected components; and

sending the datagrams node to the second node. (emphasis added)

The Applicant respectfully asserts that neither Mamros nor Patel disclose the emphasized limitation either individually or in combination.

The Mamros reference appears to disclose a protected "keepalive" message that is transmitted by a local computer to a remote computer for keeping the connection between the computers alive when the communications link between the remote and local computers has been idle. Mamros discloses a protected ISAKMP/Oakley command sent to the remote computer wherein the local computer must receive a protected acknowledgment from the remote computer so that the local computer does not terminate the communications link.

It is clear from Mamros (Col. 5, line 51 – 62) that two channels (201 and 203) are created between ISP 121 and gateway system 109. As a result two links (213 and 215) are formed between computer system 101 and gateway system 109. Mamros discloses the use of link 215 and channel 201 for control traffic for, among other things, negotiation and renegotiation of policy/key(s) for securing channels 201 and 203 (Col 5 lines 63 - Col. 6, line 7). It is further disclosed, in this section, that ISAKMP may be used to carry policy/key(s) 211 and that channel 203 may use IPSEC to carry protected data. However, Mamros does not disclose the emphasized limitation of modifying the IPSEC protected channel so as to provide for encryption of data by using only some components of the IPSEC protocol as noted in previous responses.

The Patel reference is cited for using phase 1 negotiation to establish security association between the first node and second node. However, Patel does not appear to disclose modifying the IPSEC protected channel so as to provide for encryption of data by using only some components of the IPSec protocol. (Page 6, first full paragraph, (Para. 35)) Therefore, neither Mamros nor Patel disclose the aforementioned

modification using some IPSeccomponents. This being the case, the Applicant respectfully requests the withdrawal of the rejection of claim 1.

Claims 3-4 depend from amended independent claim 1 and recite further limitations in combination with the novel elements of claim 1. Therefore, claims 3-4 contain the novel limitations of claim 1. Amended independent claim 5 is analogous to and contains limitations similar to the novel limitations of amended independent claim 1. Claims 6 and 7 depend from claim 5 and contain the same novel limitations.

Further, the Applicant respectfully submits that amended claim 7 includes limitations not disclosed in either Mamros or Patel, that of streamed data packets lacking IPSec headers. authentication headers (AH) and encapsulation security payload (ESP) headers. The Applicant respectfully requests the withdrawal of the rejection of claims 3-7.

Claim 2 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Mamros et al US 6,360,269 (hereinafter Mamros) in view of Patel et al. IP Security Working Group, Internet Draft, Intel Corporation (hereinafter Patel) and further in view of Rao, et al. US 6,757,823 (hereinafter Rao). The Applicant respectfully traverses the rejection of this claim.

The Rao reference appears to disclose a method for providing secure signaling connections for packet data network telephony calls (VOIP) using H.323 protocol. Though Rao appears to provide secure signaling connections for VOIP, Rao does not supply the missing element of modifying the IPSEC protected channel so as to only provide for encryption of data by using only some components of the IPSEC protocol.

Additionally, limitations in amended claim 2, streamed data packets lacking IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers, are not taught or suggested in Mamros, Patel or Rao. Amended claim 2 depends from amended independent claim 1 and contains the same novel limitations of claim 1. This being the case, the Applicant respectfully requests the withdrawal of the rejection of claim 2.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

By Sidney L. Weatherford
Registration No. 45,602

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8656
sidney.weatherford@ericsson.com